

# EXHIBIT 9

# Vault

A retention and eDiscovery service for organizations

Google Vault is an information governance and eDiscovery tool for Google Workspace. With Vault, you can retain, hold, search, and export users’ Google Workspace data. You can use Vault for the following data:

- Gmail messages
- Google Drive files
- Google Calendar events
- Google Chat messages (when conversation history is turned on)
- Google Meet recordings and associated chat, Q&A, and polls logs
- Google Groups messages
- Google Voice for Google Workspace text messages, voicemails and their transcripts, and call logs
- Google Sites
- Classic Hangouts messages (when conversation history turned on)

Learn more about [supported data types](#) .

## License requirements

For Vault to search and retain a user’s data, users must have a Google Workspace license and a Vault license.

Vault licenses included	Vault add-on licenses available
<ul style="list-style-type: none"><li>• Frontline Standard</li><li>• Business Plus</li><li>• <i>Enterprise Standard and Enterprise Plus</i></li><li>• All Education editions</li><li>• Enterprise Essentials and Enterprise Essentials Plus (domain-verified only)</li><li>• G Suite Business</li></ul>	For information about compatible editions, <a href="#">contact Google Sales</a> .

[Compare your edition](#)

## How licensing works

- If Vault is included with your edition, all users in your organization are automatically assigned a Vault license.
- If Vault is available as an add-on license, you can buy Vault licenses for some or all users in your organization. Only users with Vault licenses assigned to them are covered by Vault. Learn more about [how to get Google Vault](#) .
- If you delete a user or a required license, their data may be irreversibly purged and no longer available to Vault.

## Information governance: Retain and delete data

- **Keep data for as long as you need it.** If your organization is required to preserve data for a set time, you can configure Vault to retain it. Data remains available to Vault even when users delete it and empty their trash.
- **Remove data when you no longer need it.** If your organization is required to delete sensitive data after a set time, you can configure Vault to remove it from user accounts and start purging it from all Google systems.

Vault retention rules are directly applied to the data systems of supported Google services. Vault isn't a data archive. When retention rules expire, any data deleted by users or admins that isn't on hold is subject to [standard deletion processes](#). When data is purged after a retention period ends, it can't be recovered by users or admins. Learn more about [how retention works](#) .

**Note:** Vault doesn't retain data until you set up retention rules. Until you do, users can delete data and services can purge it according to that service's protocol.

## eDiscovery: Search, hold & export data of interest

With Vault, authorized users can search for data, put data on hold, and export data for further analysis.

Vault supports the first steps of the eDiscovery process outlined by the Electronic Discovery Reference Model (EDRM):

- **Identification**—You can search your organization's Google Workspace data by user account, organizational unit, date, or keyword, and preview messages, attachments, and supported files. Most services support Boolean operator searches. Learn more about [search](#) .
- **Preservation**—To preserve data indefinitely for legal or other retention obligations, you can put holds on accounts, organizational units, and groups. For Gmail and chat messages, you can also set conditions to limit the hold to messages that match. Learn about [holds](#) .
- **Collection**—After you search for data, you can export it for processing and analysis. Exports contain:
  - A comprehensive copy of all the data that matches your search criteria
  - The metadata you need to link the exported data to individual users in your organization
  - The corroborating information required to prove that the exported data matches the data stored on Google's servers.

A data export is available in Vault for 15 days, then the export is deleted to protect that data. Learn about [exports](#) .

## Access control & auditing

You can control who can access Vault and what actions are available to them. This ensures that only authorized users have access to your organization's data. Turn on Vault for select organizational units and assign the organizational units to an admin role with Vault privileges. Learn more about [controlling access to Vault](#) and [Vault privileges](#) .

Vault provides a complete audit log of user activity in Vault, including when a user creates or edits a retention rule, runs a search, or exports data. The audit log can't be edited. Learn more about [audit reports](#) .

## Get started with Vault

1. If your organization has a Google Workspace edition that doesn't include Vault, [buy Vault licenses](#) .
2. Have a Google Workspace super admin [set up Vault user access and Vault privileges](#) . They can also set up default retention rules to immediately begin retaining data. We recommend you work with your organization's legal or compliance team to determine your information governance and eDiscovery requirements.
3. Vault users can [sign in](#) and get started. For a quick start, see [Get started with Vault search and export](#) .

## Next steps

Have questions? See the [Google Vault FAQ](#) .

Running into trouble? See the [known issues](#) and track fixes and new features in [what's new](#) .

---